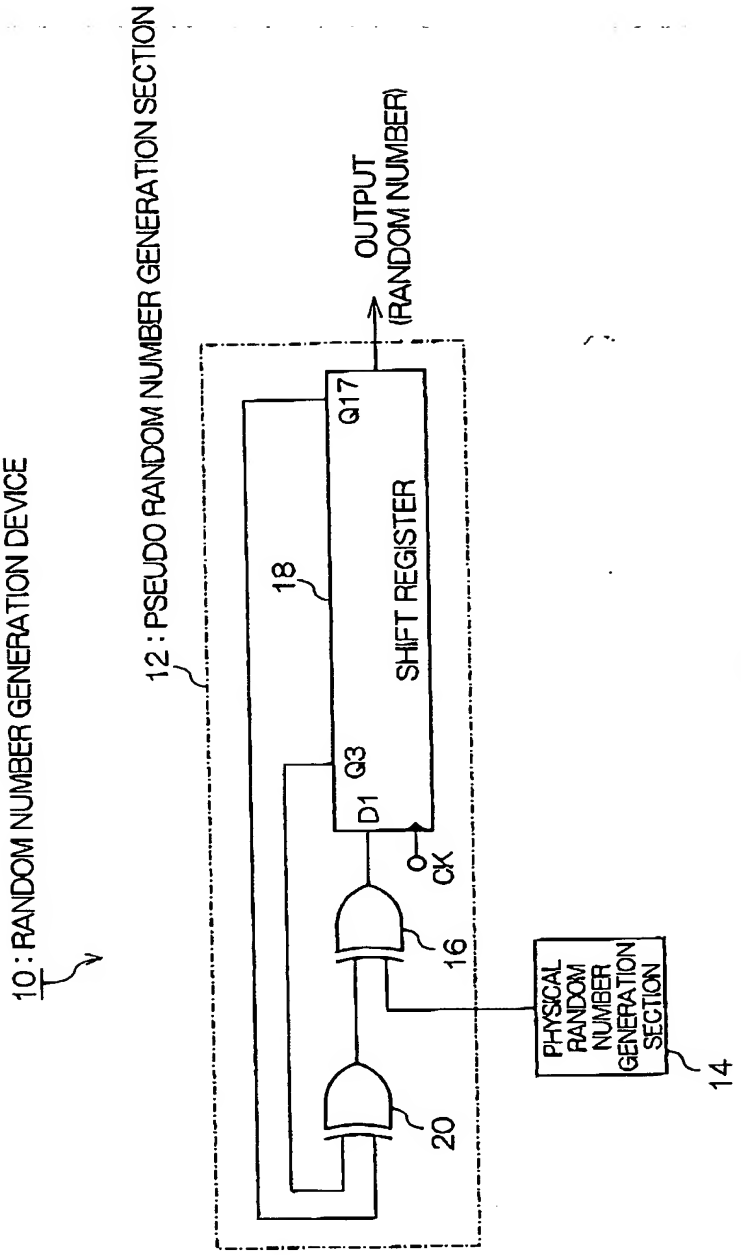
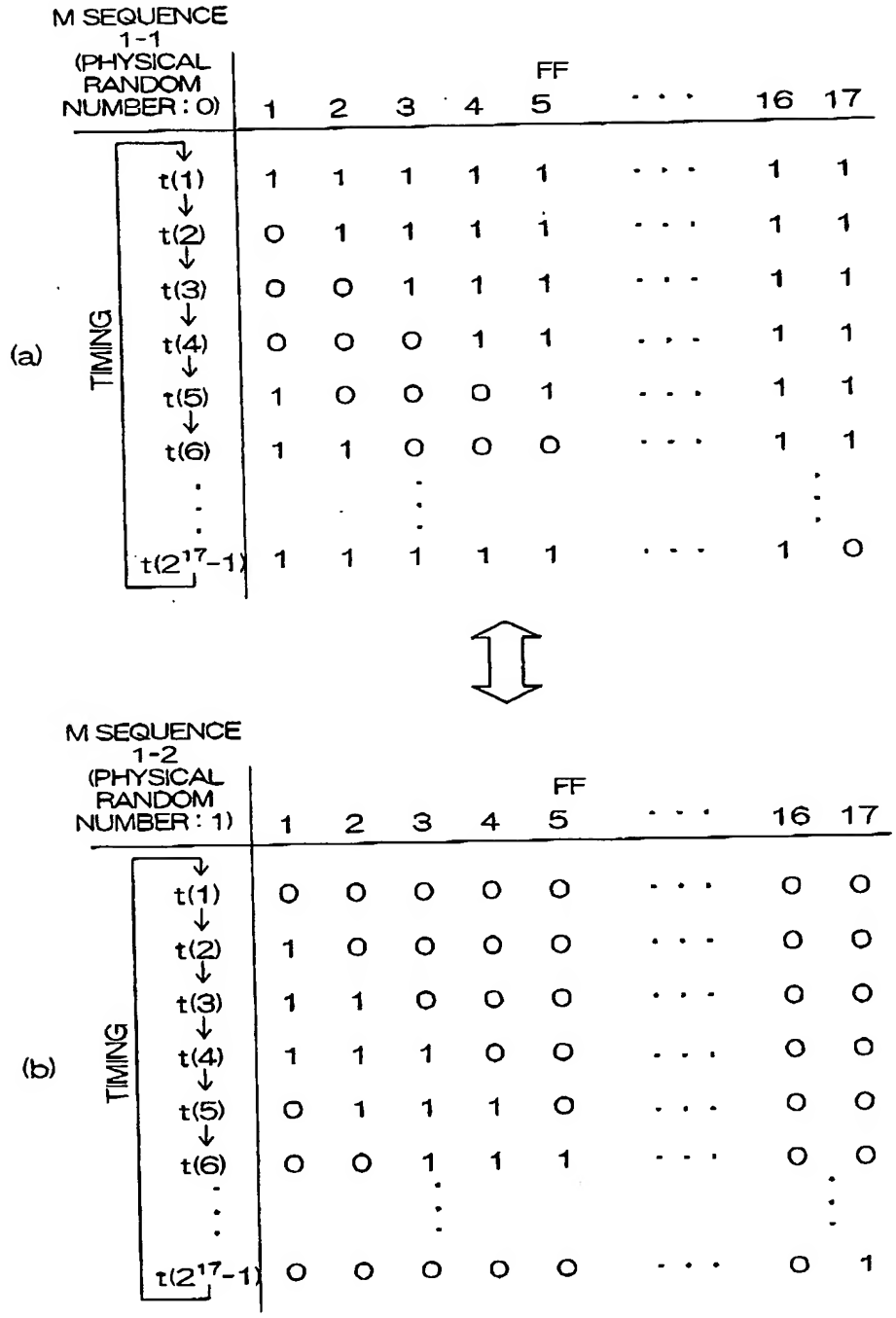

10 : RANDOM NUMBER GENERATION DEVICE
12 : PSEUDO RANDOM NUMBER GENERATION SECTION
OUTPUT
(RANDOM NUMBER)
Q17
SHIFT REGISTER
18
Q3
D1
CK
16
20
PHYSICAL
RANDOM
NUMBER
GENERATION
SECTION
14

Fig. 1

Fig. 2


(a)
M SEQUENCE 1-1 (PHYSICAL RANDOM NUMBER : 0)
FF
1 2 3 4 5 ... 16 17
TIMING
t(1) 1 1 1 1 1 ... 1 1
t(2) 0 1 1 1 1 ... 1 1
t(3) 0 0 1 1 1 ... 1 1
t(4) 0 0 0 1 1 ... 1 1
t(5) 1 0 0 0 1 ... 1 1
t(6) 1 1 0 0 0 ... 1 1
t(2^17-1) 1 1 1 1 1 ... 1 0
(b)
M SEQUENCE 1-2 (PHYSICAL RANDOM NUMBER : 1)
FF
1 2 3 4 5 ... 16 17
TIMING
t(1) 0 0 0 0 0 ... 0 0
t(2) 1 0 0 0 0 ... 0 0
t(3) 1 1 0 0 0 ... 0 0
t(4) 1 1 1 0 0 ... 0 0
t(5) 0 1 1 1 0 ... 0 0
t(6) 0 0 1 1 1 ... 0 0
t(2^17-1) 0 0 0 0 0 ... 0 1

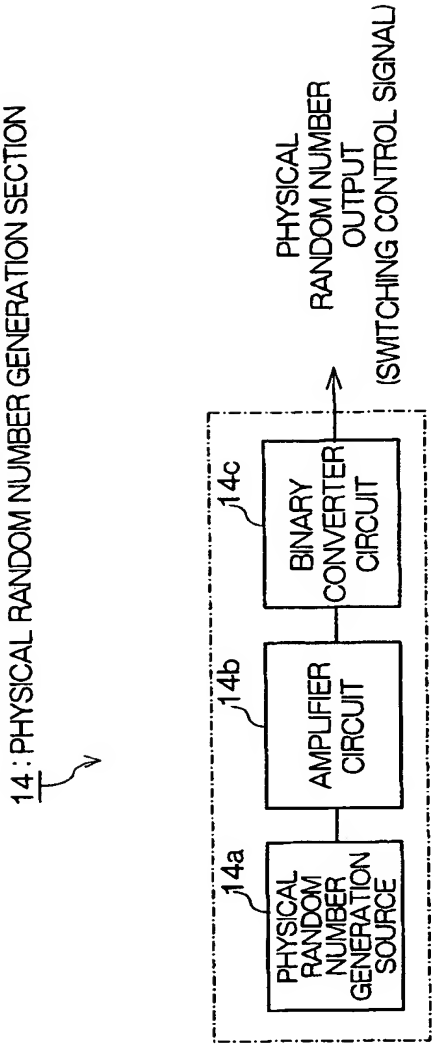

14 : PHYSICAL RANDOM NUMBER GENERATION SECTION
14a
PHYSICAL RANDOM NUMBER GENERATION SOURCE
14b
AMPLIFIER CIRCUIT
14c
BINARY CONVERTER CIRCUIT
PHYSICAL RANDOM NUMBER OUTPUT
(SWITCHING CONTROL SIGNAL)

Fig. 3

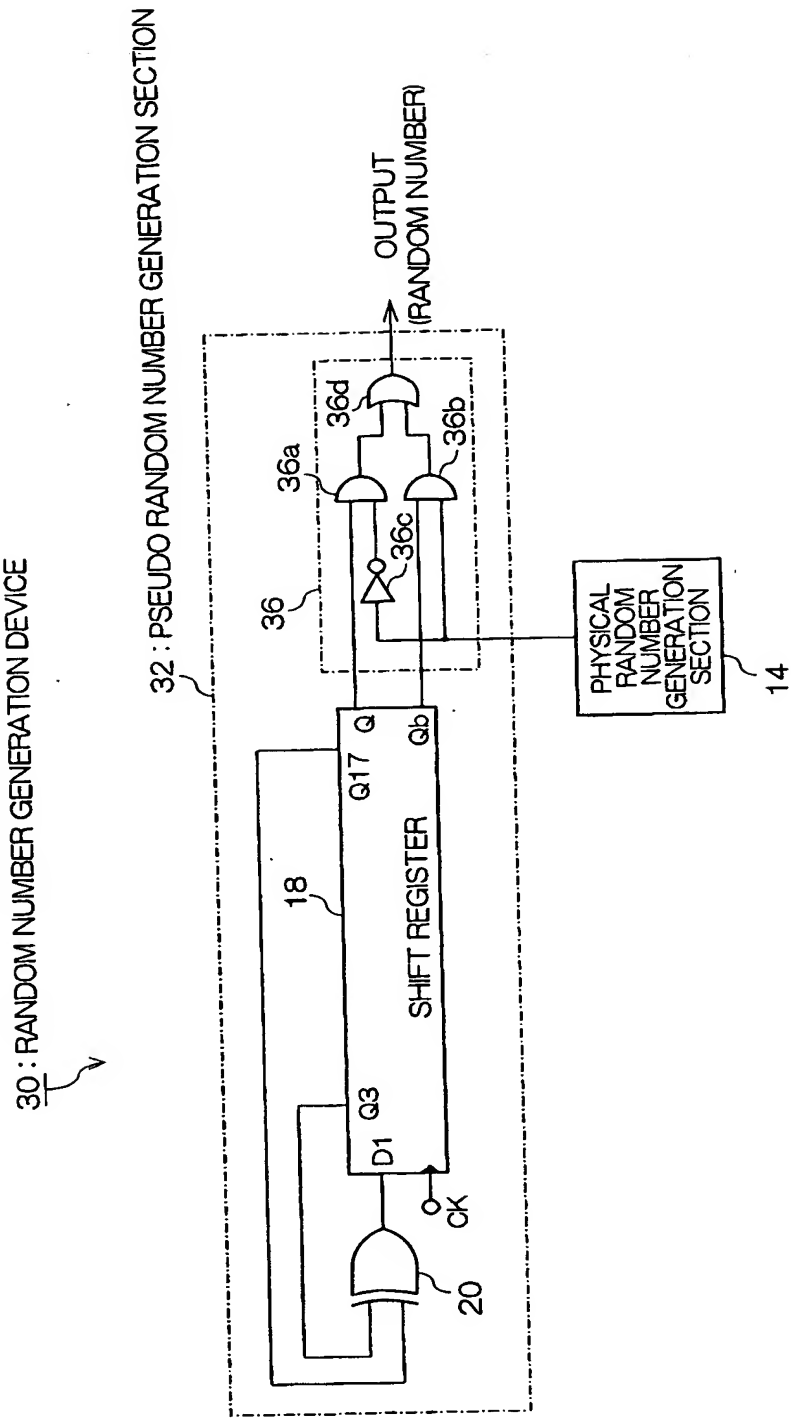

30 : RANDOM NUMBER GENERATION DEVICE
32 : PSEUDO RANDOM NUMBER GENERATION SECTION
OUTPUT (RANDOM NUMBER)
36
36a
36b
36c
36d
18
SHIFT REGISTER
Q17
Q
Qb
D1
Q3
CK
20
PHYSICAL RANDOM NUMBER GENERATION SECTION
14

Fig. 4

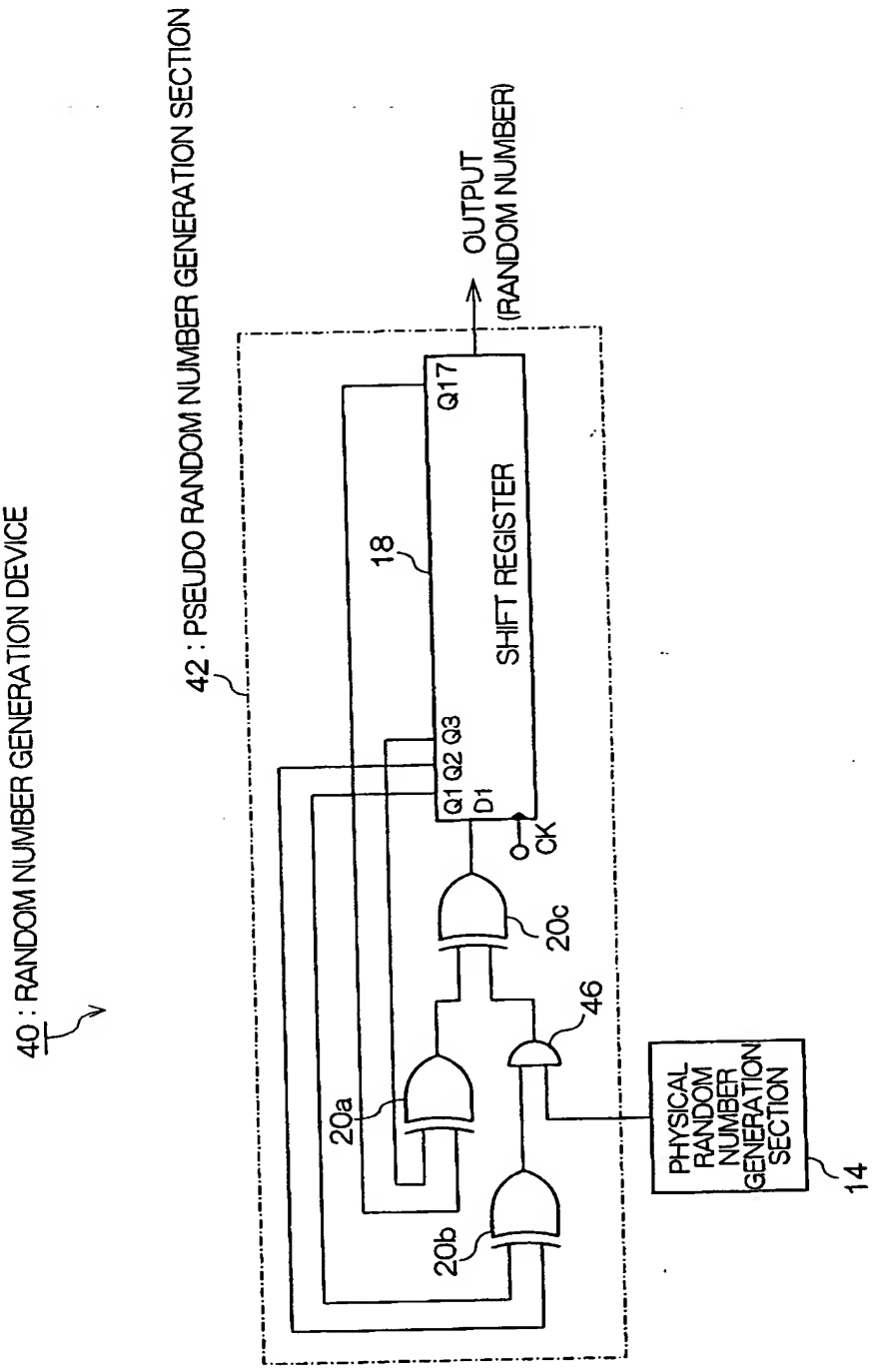

40 : RANDOM NUMBER GENERATION DEVICE
42 : PSEUDO RANDOM NUMBER GENERATION SECTION
OUTPUT
(RANDOM NUMBER)
Q17
SHIFT REGISTER
18
Q1 Q2 Q3
D1
CK
20c
46
20a
20b
PHYSICAL
RANDOM
NUMBER
GENERATION
SECTION
14

Fig. 5

Fig. 6

(a)

M SEQUENCE 3-1 (PHYSICAL RANDOM NUMBER : 0)

TIMING	FF 1	2	3	4	5	...	16	17
t(1)	1	1	1	1	1	...	1	1
t(2)	0	1	1	1	1	...	1	1
t(3)	0	0	1	1	1	...	1	1
t(4)	0	0	0	1	1	...	1	1
t(5)	1	0	0	0	1	...	1	1
t(6)	1	1	0	0	0	...	1	1
⋮	⋮		⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	...	1	0

(b)

M SEQUENCE 3-2 (PHYSICAL RANDOM NUMBER : 1)

TIMING	FF 1	2	3	4	5	...	16	17
t(1)	1	1	1	1	1	...	1	1
t(2)	0	1	1	1	1	...	1	1
t(3)	1	0	1	1	1	...	1	1
t(4)	0	1	0	1	1	...	1	1
t(5)	0	0	1	0	1	...	1	1
t(6)	1	0	0	1	0	...	1	1
⋮	⋮		⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	...	1	0

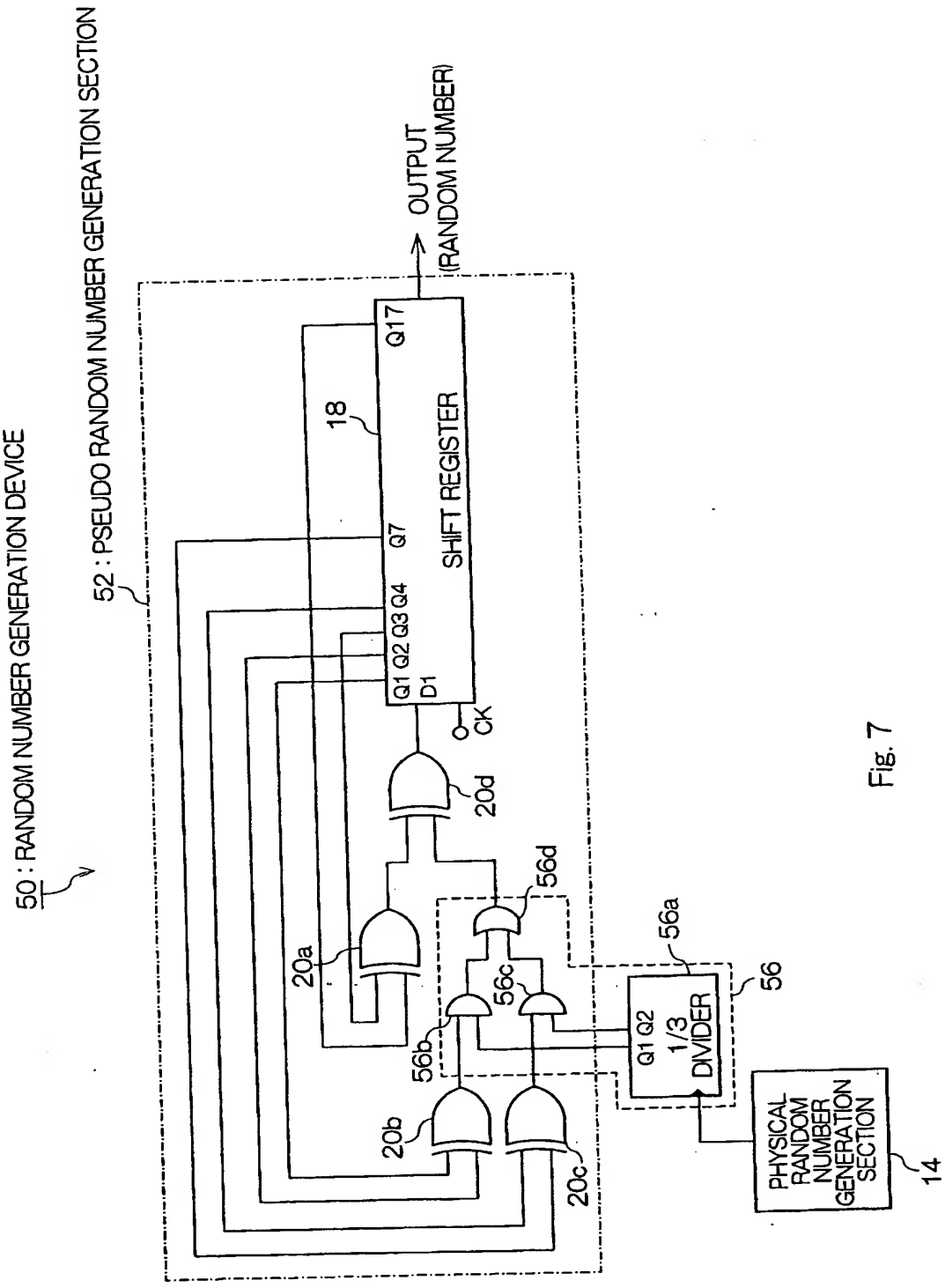

50 : RANDOM NUMBER GENERATION DEVICE
52 : PSEUDO RANDOM NUMBER GENERATION SECTION
OUTPUT (RANDOM NUMBER)
SHIFT REGISTER
Q17
Q7
Q4
Q3
Q2
Q1
D1
CK
18
20a
20b
20c
20d
56
56a
56b
56c
56d
Q1 Q2
1/3 DIVIDER
PHYSICAL RANDOM NUMBER GENERATION SECTION
14

Fig. 7

Fig. 8

(a)

M SEQUENCE 4-1 (Q1=0,Q2=0) TIMING	FF 1	2	3	4	5	...	16	17
t(1)	1	1	1	1	1	...	1	1
t(2)	0	1	1	1	1	...	1	1
t(3)	0	0	1	1	1	...	1	1
t(4)	0	0	0	1	1	...	1	1
t(5)	1	0	0	0	1	...	1	1
t(6)	1	1	0	0	0	...	1	1
⋮			⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	...	1	0

(b)

M SEQUENCE 4-2 (Q1=1,Q2=0) TIMING	FF 1	2	3	4	5	...	16	17
t(1)	1	1	1	1	1	...	1	1
t(2)	0	1	1	1	1	...	1	1
t(3)	1	0	1	1	1	...	1	1
t(4)	0	1	0	1	1	...	1	1
t(5)	0	0	1	0	1	...	1	1
t(6)	0	0	0	1	0	...	1	1
⋮			⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	...	1	0

(c)

M SEQUENCE 4-3 (Q1=0,Q2=1) TIMING	FF 1	2	3	4	5	...	16	17
t(1)	1	1	1	1	1	...	1	1
t(2)	0	1	1	1	1	...	1	1
t(3)	0	0	1	1	1	...	1	1
t(4)	0	0	0	1	1	...	1	1
t(5)	1	0	0	0	1	...	1	1
t(6)	0	1	0	0	0	...	1	1
⋮			⋮				⋮	
$t(2^{17}-1)$	1	1	1	1	1	...	1	0

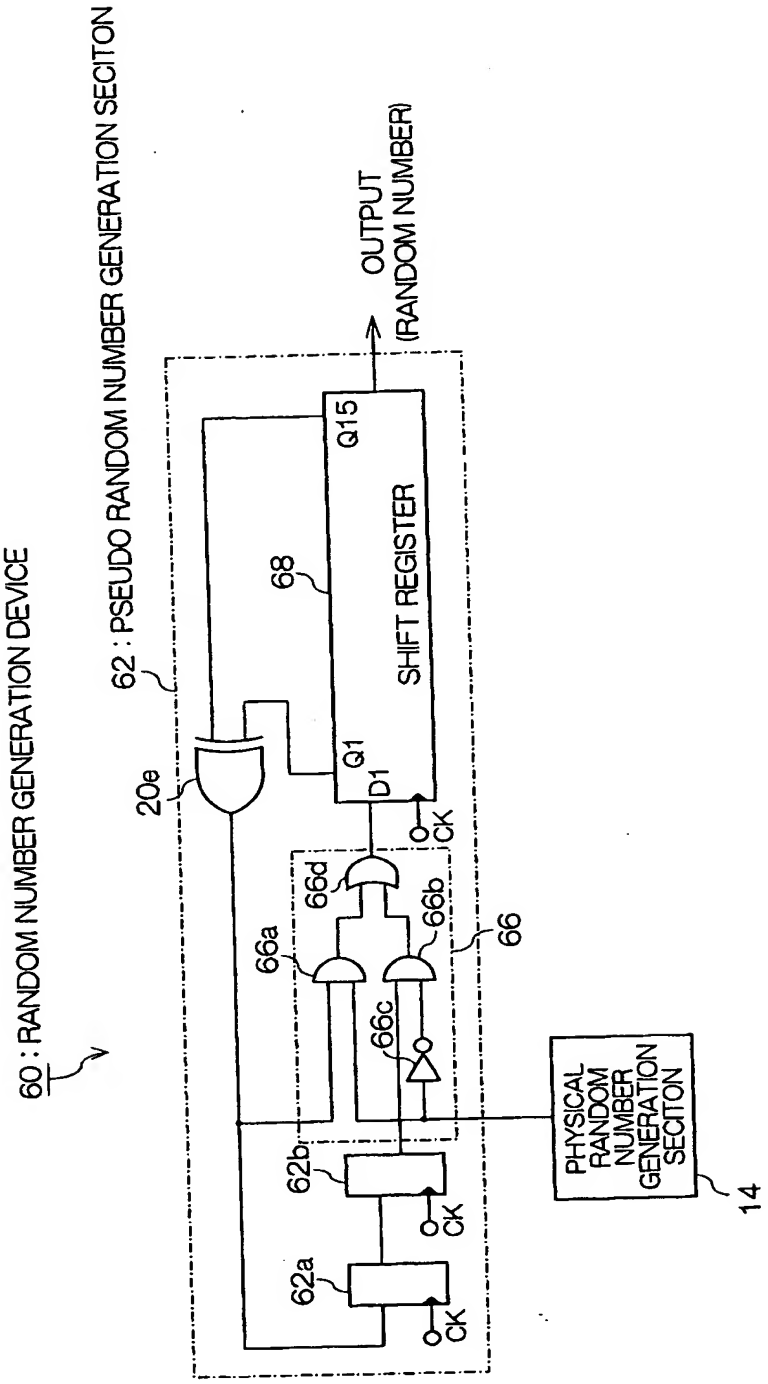

60 : RANDOM NUMBER GENERATION DEVICE
62 : PSEUDO RANDOM NUMBER GENERATION SECTION
OUTPUT (RANDOM NUMBER)
SHIFT REGISTER
Q15
Q1
D1
CK
68
20e
66
66a
66b
66c
66d
62a
62b
PHYSICAL RANDOM NUMBER GENERATION SECTION
14

Fig. 9

Fig. 10

(a)

M SEQUENCE 5-1 (PHYSICAL RANDOM NUMBER : 0)

TIMING	FF 1	2	3	4	5	...	16	17
t(1)	1	1	1	1	1	...	1	1
t(2)	0	1	1	1	1	...	1	1
t(3)	0	0	1	1	1	...	1	1
t(4)	0	0	0	1	1	...	1	1
t(5)	1	0	0	0	1	...	1	1
t(6)	1	1	0	0	0	...	1	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$t(2^{17}-1)$	1	1	1	1	1	...	1	0

(b)

M SEQUENCE 5-2 (PHYSICAL RANDOM NUMBER : 1)

TIMING	FF 1	2	3	4	5	...	14	15
t(1)	1	1	1	1	1	...	1	1
t(2)	0	1	1	1	1	...	1	1
t(3)	1	0	1	1	1	...	1	1
t(4)	0	1	0	1	1	...	1	1
t(5)	1	0	1	0	1	...	1	1
t(6)	1	1	0	1	0	...	1	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$t(2^{17}-1)$	1	1	1	1	1	...	1	0

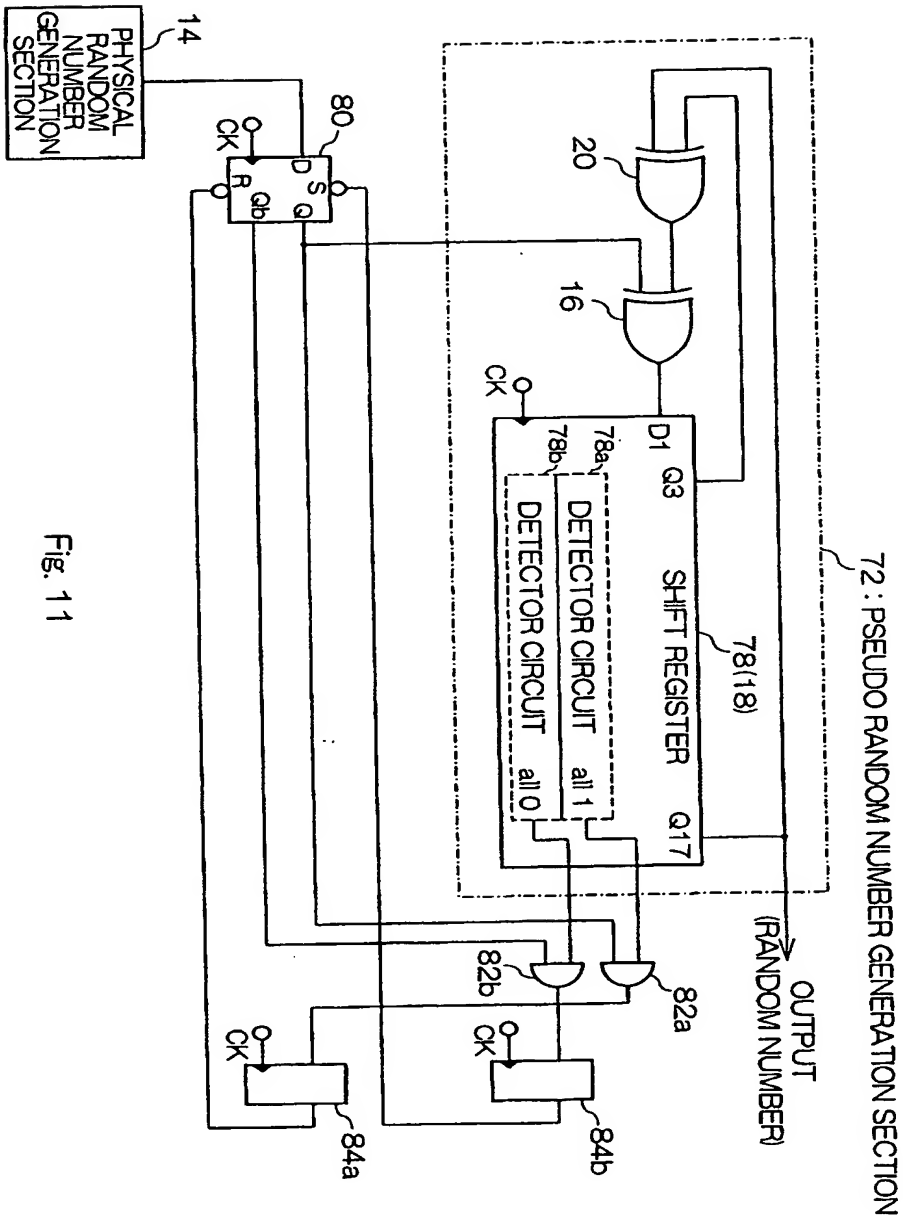

70 : RANDOM NUMBER GENERATION DEVICE
72 : PSEUDO RANDOM NUMBER GENERATION SECTION
OUTPUT (RANDOM NUMBER)
78(18)
SHIFT REGISTER
D1
Q3
Q17
78a
DETECTOR CIRCUIT all 1
78b
DETECTOR CIRCUIT all 0
20
16
CK
82a
82b
84a
84b
80
D
S
Q
R
Qb
PHYSICAL RANDOM NUMBER GENERATION SECTION
14

Fig. 11